Intel® Software Guard Extensions SDK for Linux* OS Release Notes

13 September 2018

Revision: 2.3 Open Source (version: 2.3.100.46354)

Contents:

1 Introduction

Intel provides the Intel® Software Guard Extensions (Intel® SGX) SDK, a software isolation technology, to help you protect your applications.

This document provides system requirements, installation instructions, limitations, and legal information.

Product Contents

Intel® Software Guard Extensions SDK package includes:

- An Intel® Software Guard Extensions SDK installer for Linux* OS. It includes binaries to develop enclave applications. The main components include:
    - Trusted libraries including standard C library, C++ runtime Added support, C++ STL, and others
    - Development tools including edger8r, signing tool, and others
    - Sample projects.

2 What's New

Intel® Software Guard Extensions SDK includes the following changes in version 2.3:

- Added support for Ubuntu* 18.04 LTS 64-bit Desktop and Server version

- Provided a new set of the SGX common loader APIs in sgx_enclave_common.h
- Provided the sample code for Switchless Call
- Provided a new API in tcrypto: `sgx_ecc256_calculate_pub_from_priv`
- Changed the `sgx_create_enclave` API: the function ignores the parameter of a launch token and will not update it after the function successfully returns
- Fixed bugs.

Changes in Previous Releases

Intel® Software Guard Extensions SDK includes the following changes in version 2.2:

- Added support for Switchless, a new mode of operation to perform calls from/to SGX enclaves
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.3:

- Updated the cryptography library to Intel® Integrated Performance Primitives Cryptography 2018 Update 2.1. Mitigated security vulnerability CVE-2018-3617 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3617). For more details, refer to Security Advisory INTEL-SA-00106 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00106&languageid=en-fr) and INTEL-SA-00135 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00135&languageid=en-fr)
- Provided enhancements to the Intel® SGX Cryptographic library
- Added support for Intel® SGX Protected Code Loader (Intel® SGX PCL). It is intended to protect Intellectual Property (IP) within the code for Intel® SGX enclave applications
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.2:

- Mitigated security vulnerability CVE-2018-3626 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626). For more details, refer to Security Advisory INTEL-SA-00117 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00117&languageid=en-fr)

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.1:

- Updated security to the Intel® SGX SDK
- Added new `sgx_register_wl_cert_chain` API that allows the Intel® SGX application to register an enclave
- Added support for CentOS* 7.4
- Added support for SUSE* Linux Enterprise Server 12
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.0:

- Added support for the Intel® SGX Enclave Dynamic Memory Management (EDMM) to dynamically manage enclave memory: dynamic heap expansion, dynamic stack expansion, dynamic thread creation, and page attribute modification
- Added support for Red Hat* Enterprise Linux* Server 7.4
- Added support for Safe String APIs of the C library in an enclave
- Added an option to build the Intel® SGX SDK using the Intel® SGX SSL crypto library instead of the Intel® IPP Cryptography open source version
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.9.100.39124:

- Added C++11 Added support

  To improve support for C++11 on the Linux* OS, the Linux* SDK 1.9 includes a new trusted C++ library based on libc++ (see http://llvm.org/svn/llvm-project/libcxx/trunk). Note that the Standard C++ Library based on STLPort (sgx_tstdcxx) will be deprecated in the next release.

- Added support for Protected File System – a basic subset of the regular 'C' file API for Intel® SGX enclaves that provides files with both confidentiality and integrity protection
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.8.100.37689:

- Added support for the TCMalloc library

- Added support for new Linux* distributions. See Software Requirements for details
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.7.100.36470:

- Updated the cryptography for Intel® Integrated Performance Primitives (Intel® IPP) library to version 9.0 Update 4
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.6.100.34478:

- Added new `setjmp/longjmp` APIs in the trusted C library
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes before version 1.5.100.32783:

- Added support for profiling Intel® SGX applications using the Intel® VTune™ Amplifier. To profile Intel® SGX applications, use the VTune™ Amplifier 2016 Update 2, the "Intel SGX Hotspots" analysis type.
- Added the Intel® SGX Eclipse* plug-in to create Intel® SGX enclave projects
- Added support for implicit Thread Local Storage (TLS)
- Added support for nested HW exception in a trusted environment

3 System Requirements

Software Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 16.04 LTS 64-bit Desktop and Server version
    - Ubuntu* 18.04 LTS 64-bit Desktop and Server version
    - Red Hat* Enterprise Linux* Server 7.4 (for x86_64)
    - CentOS* 7.5 (for x86_64)

- SUSE* Enterprise Server 12 (for x86_64)
- Fedora* 27 Server version

NOTE: It is highly recommended to use the listed Linux* OS distributions. Other distributions have not been tested.

4 Known Issues and Limitations

- Intel® SGX for Linux* OS does not support setting a different charset in GNU* Project Debugger (GDB*).
- Building the Intel® SGX SDK sample project "RemoteAttestation" is possible only within the Intel® SGX SDK installation folder.
- Intel® SGX does not support the "long long" type in C++ templates.
- `sgx-gdb` depends on GDB* 7.9.1 or later versions. Please upgrade GDB* if its version is lower than 7.9.1.

5 Disclaimer and Legal Information

Optimization Notice

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Notice revision #20110804